

Gia Lai: Cảnh báo thủ đoạn giả mạo sàn thương mại điện tử, lừa đảo “săn sale” dịp cuối năm

16:21 24/10/2026

Trước thềm các đợt mua sắm trực tuyến lớn dịp cuối năm như 11/11 và 12/12, Công an tỉnh Gia Lai vừa phát đi cảnh báo người dân cần nâng cao cảnh giác trước các thủ đoạn giả mạo sàn thương mại điện tử, đơn vị vận chuyển và nhân viên chăm sóc khách hàng nhằm đánh cắp thông tin tài khoản, chiếm đoạt tài sản.

Theo Công an tỉnh Gia Lai, thời điểm cuối năm gắn liền với các ngày hội mua sắm trực tuyến lớn luôn đi kèm hàng loạt chương trình giảm giá sâu, mã ưu đãi và hoàn tiền được quảng bá rầm rộ trên không gian mạng. Lợi dụng nhu cầu tiêu dùng tăng cao cùng tâm lý muốn săn hàng giá rẻ, sợ bỏ lỡ cơ hội của người dân, các đối tượng tội phạm công nghệ cao đã triển khai nhiều kịch bản tinh vi để tiếp cận, dẫn dụ người mua chuyển tiền hoặc cung cấp thông tin bảo mật.

Nhận diện các kịch bản lừa đảo từ “giảm giá sốc” đến hoàn tiền đơn hàng

Một trong những phương thức phổ biến nhất hiện nay là việc các đối tượng tạo lập các trang web, fanpage, tài khoản mạng xã hội hoặc gian hàng trực tuyến giả mạo, sao chép tương đồng tên gọi, hình ảnh và logo của các thương hiệu lớn hoặc sàn thương mại điện tử uy tín. Để đánh vào tâm lý người mua, các trang giả mạo này liên tục tung ra những thông điệp quảng cáo như “sale 90%”, “xả kho hàng chính hãng giá sốc”, “voucher độc quyền chỉ áp dụng trong hôm nay” nhằm tạo cảm giác khẩn cấp, thúc giục khách hàng chốt đơn khi chưa kịp kiểm chứng thông tin. Khi người dân liên hệ, các đối tượng lập tức yêu cầu chuyển khoản đặt cọc hoặc thanh toán trước bên ngoài nền tảng với lý do giữ hàng, giữ giá ưu đãi, sau đó nhanh chóng chặn liên lạc chiếm đoạt tiền hoặc viện cớ lỗi hệ thống để yêu cầu nạn nhân chuyển thêm tiền.

Tinh vi hơn, các đối tượng còn mạo danh nhân viên chăm sóc khách hàng của sàn thương mại điện tử, chủ gian hàng hoặc nhân viên giao hàng để liên hệ với người mua, thông báo đơn hàng gặp sự cố, thanh toán nhầm, giao sai sản phẩm

hoặc lỗi áp dụng mã giảm giá cần làm thủ tục hoàn tiền. Tiếp đó, chúng gửi kèm các đường dẫn (link) lạ, mã QR hoặc hướng dẫn nạn nhân thực hiện các thao tác kỹ thuật nhằm thu thập thông tin thẻ ngân hàng, mật khẩu và mã xác thực (OTP). Ngoài ra, chiêu thức thông báo trúng thưởng “quà tri ân”, “khách hàng may mắn”, “voucher nội bộ” hay “nâng hạng thành viên” cũng được sử dụng thường xuyên để lôi kéo người dân đóng các khoản phí kích hoạt, phí vận chuyển hoặc tiền thuế trước khi nhận quà.



Ảnh minh họa. Hình ảnh do AI tạo ra

Tuyệt đối không giao dịch ngoài nền tảng và bảo mật mã xác thực

Trước các thủ đoạn ngày càng biến tướng, Công an tỉnh Gia Lai khuyến cáo người dân cần đặc biệt cảnh giác trước những mặt hàng rao bán với mức giá rẻ bất thường kèm yêu cầu chuyển khoản trực tiếp ngoài hệ thống thanh toán của sàn thương mại điện tử. Người tiêu dùng tuyệt đối không truy cập vào các đường dẫn lạ, không quét mã QR không rõ nguồn gốc được gửi qua tin nhắn và không thực hiện giao dịch chỉ vì những lời hối thúc như “ưu đãi sắp hết”, “đơn hàng sắp bị hủy” hay “tài khoản sắp bị khóa”. Đặc biệt, trong mọi tình huống, người dân tuyệt đối không cung cấp mật khẩu, mã PIN, mã OTP, thông tin thẻ ngân hàng hoặc chia sẻ màn hình điện thoại cho bất kỳ ai tự xưng là nhân viên sàn thương mại điện tử, ngân hàng hay đơn vị vận chuyển.

Để bảo đảm an toàn trong mùa mua sắm cuối năm, người dân chỉ nên giao dịch trên các ứng dụng, website và gian hàng chính thức đã được xác thực; kiểm tra kỹ tên miền trang web, lịch sử hoạt động và đánh giá của người mua trước khi thanh toán. Khi nhận được thông báo bất thường về đơn hàng, người mua cần chủ động mở ứng dụng chính thức của sàn thương mại điện tử để kiểm tra trạng

thái đơn hàng hoặc liên hệ trực tiếp tới tổng đài chăm sóc khách hàng được công bố chính thức, tuyệt đối không cài đặt các ứng dụng lạ theo hướng dẫn của người không quen biết.

Trường hợp phát hiện dấu hiệu lừa đảo hoặc đã trót thực hiện giao dịch đáng ngờ, người dân cần khẩn trương liên hệ với ngân hàng hoặc tổ chức cung ứng dịch vụ thanh toán để yêu cầu phong tỏa, ngăn chặn giao dịch; đồng thời lưu giữ toàn bộ bằng chứng gồm số điện thoại, số tài khoản thụ hưởng, địa chỉ website, tin nhắn trao đổi và biên lai chuyển tiền để trình báo cơ quan Công an gần nhất xử lý theo quy định.

Thành Nam